UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

3015 E Wendover Avenue,
Greensboro, North Carolina 27405

Case No. 1:20mj140

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

the entire premises located at 3015 E Wendover Avenue, Greensboro, North Carolina 27405.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See attachment A.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. § 2252A(a)(2)(A)	Distribution of Child Pornography

The application is based on these facts:

Please see the attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Emily R. Keller
Applicant's signature

FBI Special Agent Emily R. Keller
Printed name and title

Sworn to before me and signed in my presence.

Date: 05/27/20

Judge's signature

City and state: Greensboro, North Carolina

L. Patrick Auld, United States Magistrate Judge
Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire premises located at 3015 E Wendover Avenue, Greensboro, North Carolina 27405 (the SUBJECT PREMISES). The residence is a one-story single-family home with light gray siding and a rear shed. The numbers "3015" are prominently displayed by the front door. The property is listed in Guilford County GIS as deed book 8133 page 1959, parcel number 21881.

ATTACHMENT C

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B):

1. Computers or storage media that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored.
2. Routers, modems, and network equipment used to connect computers to the Internet.
3. Child pornography, as defined in 18 U.S.C. 2256(8).
4. Child erotica.
5. Records, information, and items relating to violations of the statutes described above in the form of:
    a. Records and information referencing child pornography, as defined in 18 U.S.C. 2256(8), and/or child erotica;
    b. Records, information, and items referencing or revealing the occupancy or ownership of 3015 E Wendover Avenue, Greensboro, North Carolina 27405, including utility and telephone bills, mail envelopes, or addressed correspondence;
    c. Records and information referencing or revealing access to and/or use of Kik Messenger;

d. Records and information referencing or revealing the use of the handle "chris32033", or any variant thereof, and the identity of the user;

e. Records and information referencing or revealing the owner or user of an iPhone at the SUBJECT PREMISES;

f. Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;

g. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence such as social media sites or applications containing groups or chat rooms dedicated to accessing child pornography, to include Kik, Facebook, Tumblr, and Shutterbug as well as online repositories known to be accessed with the intent to view child pornography such as Imjur and TOR

h. Records and information referencing or revealing the use of remote computing services such as email, cloud storage, or online social media services; and

i. Records and information referencing minors "Payton" or "Zakk" and/or revealing their identities.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, deleted, viewed, or otherwise interacted with;

b. evidence of how and when the COMPUTER was used to create, edit, delete, view, or otherwise interact with or access child pornography or share child pornography with others;

c. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

d. evidence of the Internet Protocol addresses used by the COMPUTER;

e. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

f. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

g. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

h. evidence of the lack of such malicious software;

i. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

7. During the course of the search, photographs of the location to be searched may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form

(such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Emily R. Keller, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am investigating offenses related to child sexual exploitation. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 3015 E Wendover Avenue, Greensboro, North Carolina 27405 (the "SUBJECT PREMISES"), more specifically described in Attachment A, and the person of Christopher Dean HALL (the "SUBJECT PERSON"), as more specifically described in Attachment B, for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B), which items are more specifically described in Attachment C.

2. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and

evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located at the SUBJECT PREMISES and/or on the SUBJECT PERSON.

AFFIANT BACKGROUND

3. I am a Special Agent of the Federal Bureau of Investigation ("FBI"), and have been since October of 2019. My initial training consisted of an eighteen-week FBI new agent course during which I received instruction on various aspects of federal investigations, ranging from economic espionage and child pornography, to kidnapping and computer intrusions. In addition, I have earned both a Bachelor of Arts in International Studies and a Master of Public and International Affairs. I am currently assigned to the Charlotte Division and stationed at the Greensboro Resident Agency. As I am new to investigations involving child exploitation and child pornography, FBI Special Agent Tara S. Thomas, who has investigated child pornography cases for more than eight years, assisted me with drafting this Affidavit. Prior to becoming a Special Agent of the FBI, I worked as a Staff Operations Specialist, investigative analyst, for the FBI for over four years. I have supported numerous FBI investigations through investigative research and analysis, to include investigations of cybercrime. I am familiar with, and have employed,

investigative techniques used in these investigations, such as analysis of Internet Protocol addresses and Internet Service Provider records. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2252A, and I am authorized by law to request a search warrant. As a Special Agent, I am authorized to investigate violations of laws and to execute warrants issued under the authority of the United States.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).

b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18

U.S.C. § 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(2).

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment C:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors

but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips,

and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. A "Hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

k. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

l. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

o. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. "Remote computing service", as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

r. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

s. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON KIK MESSENGER

6. Kik Messenger (hereinafter "Kik") is a mobile application designed for chatting or messaging owned and operated by MediaLab.AI, Inc., a United

States based holding company of Internet brands. Kik was formerly owned by Kik Interactive, Inc., a Canadian based company. MediaLab.AI, Inc., acquired the Kik application in October 2019.

7. According to "Kik's Guide for Law Enforcement," published in July 2019, to use the Kik application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user is asked to supply an email address, however, the email address does not have to be verified in order to use the application. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

8. According to "Kik's Guide for Law Enforcement," Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text messages, images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that

includes all of their contacts or any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.

PROBABLE CAUSE

9. On April 15, 2020, an FBI undercover agent, known as an "Online Covert Employee" (OCE) interacted with an individual using the Kik username, "chris32033", subsequently identified as HALL through investigative means detailed below, on two different platforms. Kik user "chris32033" was interacting in a Kik chat group utilized by individuals to discuss and trade child sexual exploitation material. User "chris32033" identified himself as a 35 year old male from the United States while he was in the chat group. After Kik user "chris32033" informed another member in the chat group that he had sexual intercourse with his son who "chris32033" purported to be 13 years old, the OCE sent a private message to user "chris32033" to begin chatting with user "chris32033" as further described below.

10. On April 15, 2020, the OCE entered Kik chat group #dadboysangel. At this time, the OCE noticed "chris32033" informed another chat group member that "chris32033" had sexual intercourse with his son. At 1:30 p.m.,

the OCE sent a private message to "chris32033" and began chatting with "chris32033" to ascertain whether he had access to children, and if so, whether he was sexually abusing them. The OCE asked, "U a real dad or fantasy/rp?" and "chris32033" responded with "Real dad he is 13 you?" The OCE replied that he had a 12 year-old daughter. The OCE questioned "chris32033" as to whether his son is shy. Kik user "chris32033" responded with "Nah we always been nude together. I'm bit of nudists and when he visits we were always nude started young and very slow." During the conversation, "chris32033" said he engaged in sexual intercourse with his purported son's friends who were also minors. The OCE said, "How far have you gone? Looking to kind of know the pace that is normal." Kik user "chris32033" said, "We fuck each other and suck etc and last year his two best friends came a week during the summer I had him."

11. Kik user "chris32033" told the OCE that he does not have custody of his son but that his son visits for two to three weeks in the summer and on certain holidays. Kik user "chris32033" suggested he and his son meet with the OCE and his daughter. Kik user "chris32033" said, "But be hot to hang the four of us bet my boy would love to meet your girl." Kik user "chris32033" told the OCE that he lived in North Carolina. Kik user "chris32033" told the OCE that his son lives in South Carolina and was approximately five hours away from

"chris32033." Kik user "chris32033" asked the OCE to "Imagine watching our kids fucking." In reply, the OCE explained that he and his daughter may be able to meet up with "chris32033" and his son. Kik user "chris32033" made several suggestions regarding the type of lodging and specifically said it should be remote stating "Gotcha I'm down for whatever but we can be more nude and open in a house or cabin then hotel room." Kik user "chris32033" and the OCE discussed the sexual activities they would want to perform with their purported children. Kik user "chris32033" told the OCE, "She prob would like mine I'm sure lol", referring to his son and the OCE's daughter. When the OCE asked "chris32033", "Think he'd be into it?", "chris32033" responded, "Oh I'm sure he would. He loves to fuck I mean he fucks his gf with his buddies." The OCE replied, "He'd have to be nice bc she hasn't ever been fucked." Kik user "chris32033" later asked the OCE, "I know but what would you want to happen after seeing my boys cock slide in and out of her tight virgin pussy. You get naked and jerk, or you get behind my boy and slide your dad cock in his smooth hole." The OCE asked "chris32033" for a picture of his son that he could show his daughter. Kik user "chris32033" sent the OCE an image of a young white male whose appearance is consistent with a 13 year old. At 3:51 p.m., after the OCE and "chris32033" exchanged a few more messages, the Kik private message was terminated.

12. On April 16, 2020 at 12:04 p.m., the OCE interacted with "chris32033" on Kik again via private message. Kik user "chris32033" asked if the OCE showed his son's image to the OCE's daughter. Kik user "chris32033" asked for a photo of the OCE's daughter. The OCE sent an image that was not an actual child. Kik user "chris32033" said he sent the image to his purported son, Payton, who expressed an interest in having sex with the OCE's daughter.

13. The OCE asked if "chris32033" had any videos in his collection but did not indicate the videos should contain children or pornography. The OCE indicated "chris32033" should not just search the internet for videos. Kik user "chris32033" said he "mostly have boys stuff" and he subsequently sent three videos to the OCE. The children in all three videos were clearly minors that were engaged in sexual conduct as defined by statute. The OCE questioned how "chris32033" received the videos and "chris32033" replied, "someone sent them to me."

14. On April 16, 2020, an administrative subpoena was issued to Kik for subscriber information for user "chris32033." In response to the subpoena, Kik provided the following:

First name:	Chris
Last Name:	h
Email:	chris32033@yahoo.com (unconfirmed)
Registration	Timestamp: 01/20/2013 at 09:17 p.m.
Device:	iPhone

15. Kik IP address records logged user "chris32033" using the IP address 104.188.162.252 eight times on April 15, 2020 between 1:30 p.m. and 3:51 p.m. A query of the American Registry for Internet Numbers ("ARIN") online database revealed IP address 104.188.162.252 as being registered to AT&T Internet Services.

16. On May 20, 2020, an administrative subpoena was issued to AT&T Internet Services for account subscriber information associated with IP address 104.188.162.252. As a result of the subpoena, AT&T Internet Services, provided the following account information:

Subscriber Name:	Chauncey Brummell
Subscriber Address:	3015 E Wendover Avenue, Greensboro, North Carolina 27405
Email:	chaunceybrummell@gmail.com

17. The AT&T Internet Services, records indicate that IP address 104.188.162.252 was assigned to the account of Chauncey Brummell from March 30, 2020 to April 30, 2020.

18. On May 21, 2020, I observed the residence located at the SUBJECT PREMISES. The residence is a one-story single-family home with light gray siding and a rear shed. The numbers "3015" are prominently displayed above the front door. The property is listed in Guilford County GIS as deed book 8133 page 1959, parcel number 21881.

19. A check of publicly available databases show Chauncey Brummell, date of birth 04/19/1979, and Christopher HALL, date of birth 03/27/1985, as living at the SUBJECT PREMISES. On May 21, 2020, I observed two vehicles at the SUBJECT PREMISES, one of which was registered to HALL. Another vehicle at the residence was registered to Chauncey Brummell.

20. Upon receipt of this information, an FBI analyst used available open source databases to identify HALL as a visual arts teacher at Gate City Charter Academy in Greensboro, North Carolina. HALL also manages a photography and graphic design business. The associated business card listed the email address for the business as chris32033@yahoo.com. HALL appears to use the moniker "chris32033" for multiple other social media pages such as Pinterest and Shutterbug. The Facebook page for HALL contains the same black and white photograph, of a middle-aged white male with dark hair, used in the Kik user "chris32033" account.

21. The image that "chris32033" sent to the OCE of his purported son bears physical similarity to a child identified as "Zakk", possibly the nephew of HALL. The images were located on HALL's photography Facebook page under "Zakk's Birthday." Zakk appears to be the son of Amber Allred and Dustin Allred. Dustin married HALL's sister, Shaina Allred in 2013.

22. On May 19, 2020, I reviewed the three videos "chris32033" sent to the OCE over Kik Messenger. The following is a brief description of the three videos:

a. "IMG_0325" is an MP4 lasting 46 seconds long and depicts a young child's room with a bed and desk. There is a picture on the wall in a different language other than English, perhaps Arabic. A prepubescent male child about the age of 5 years old is lying facedown on the bed wearing a grey hoodie and no pants. A post-pubescent male about the age of 16 years old wearing black glasses and a red and black shirt enters the video frame. His black pants are pulled down exposing what appears to be an erect penis. He then penetrates the child anally with his penis. The child appears to be in distress as he smothers his face in the pillow and also hits the pillow with his fist multiple times. Based on my training and experience, this video can be classified as Bondage, Discipline, Sadism, and Masochism (BDSM).

b. "IMG_0326" is an MP4 one minute and 58 seconds long and depicts a room with white walls, a desk chair, and a red sofa in the background. Another person (unknown age as only the arm is seen) is on the sofa playing with the sofa pillows. A prepubescent female child about the

age of six years old with brown hair is nude lying on top of a nude uncircumcised adult male. The child is using her mouth and hands to provide sexual pleasure to the adult male. The child's eyes are wide, and she appears to be tired and pulls the penis out of her mouth to breathe a few times.

c. "IMG_0326" is an MP4 lasting 37 seconds and depicts a prepubescent male about the age of five years old asleep or otherwise unconscious and wearing a black shirt or pajamas with an orange zipper. An adult male with what appears to be an erect penis uses his left hand to masturbate on the child's face and penetrates the child's mouth with the tip of the penis. The adult male is using his hand to move his penis and stimulate his penis. The child never appears to awaken.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

23. I have had both training and experience in the investigation of computer-related crimes, as well as that of other agents assisting in the investigation. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and computers with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced,

distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or

electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Such an account can also be accessed in the same way. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite

websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

i. Individuals involved in the receipt, possession, and/or distribution of child pornography very frequently possess multiple devices that contain evidence of their interaction with child pornography and/or sexual interest in minors. In modern American culture, most individuals possess multiple devices that have the ability to connect to the Internet (e.g., tablets, desktop computers, laptop computers, and mobile phones). Many individuals also keep prior versions of their devices (e.g., prior cell phones and prior computers). This is the case because (1) individuals are often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction and prior versions can often be used until the current device is repaired or replaced.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

24. As described above and in Attachment C, this application seeks permission to search for records that might be found at the SUBJECT PREMISES or on the SUBJECT PERSON, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

25. I submit that if a computer or storage medium is found at the SUBJECT PREMISES and/or on the SUBJECT PERSON, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or

even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

26. As further described in Attachment C, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the SUBJECT PREMISES and/or on the SUBJECT PERSON because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices

or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the

computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's

state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer

behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

27. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users

can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

28. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for

both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

29. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

30. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment C, are located at the SUBJECT PREMISES, more fully described in Attachment A, and/or on the SUBJECT PERSON, more fully described in Attachment B. I, therefore, respectfully request that the attached warrant be issued authorizing the search of the SUBJECT PREMISES and the SUBJECT PERSON and the seizure of the items listed in Attachment C.

Emily R. Keller
Special Agent
Federal Bureau of Investigations

Sworn and subscribed before me this 27th day of May, 2020.

L. Patrick Auld
United States Magistrate Judge